FOR YOUR INFORMATION

Summer 2009

Medicaid Electronic Health Record System and e-Prescribing System

By Cheryl Crawford, MEHRS/eScript Project Manager
Mississippi Division of Medicaid

For many years, the Division of Medicaid (DOM) has been aware of the need for a combined Medicaid Electronic Health Records System and statewide e-prescribing system. In Mississippi, health care is delivered by a variety of providers working in a large array of inpatient and ambulatory settings, who utilize different technologies with no clearly defined interoperability. Medicaid providers find it challenging to obtain complete health care information on beneficiaries, which adversely affects their ability to provide beneficial treatment. The Medicaid Electronic Health Record System and e-Prescribing System (MEHRS/eScript) will assist providers and others by providing point of service web-based access to beneficiary claims history including encounter data and medication history. The project to design, develop and implement MEHRS/eScript was begun on July 1, 2009 via a contractual agreement between DOM and Shared Health, Inc.

The contract phases are:

1. Initial Design, Development and Implementation (DDI) Phase (Phase 1), to be completed by 12/31/2009.
   a. Web portal access for Medicaid providers to obtain an electronic health record based on Medicaid medical and prescription claims data
   b. Web-based e-prescribing system using Medicaid claims data
   c. Web portal access for Medicaid providers to obtain hospital discharge information based on Medicaid claims
2. Operational Phase.
3. Enhancement Phase (Phase 2 and 3), timeframes to be determined.
   a. Implement web portal access for Medicaid providers to obtain laboratory test results and x-rays in the web portal (Phase 2)
   b. Implement ability to participate in a Regional Health Information Organization (RHIO) to receive Electronic Medical Records (EMR) and to send and receive EHR (Phase 2)
   c. Implement web portal access for beneficiaries to view/update personal health information (Phase 3)
   d. Implement functionality to allow other payers to participate (Phase 3)
4. Turnover Phase.

INSIDE THIS ISSUE

National Broadband Mapping Program

By Craig P. Orgeron, Ph.D.
Director, Strategic Services

The State Broadband Data and Development Grant Program is a competitive, merit-based matching grant program that implements the joint purposes of the American Recovery and Reinvestment Act and the Broadband Data Improvement Act (BDIA), and is administered by the Department of Commerce's National Telecommunications and Information Administration (NTIA).

The Program will provide up to approximately $240 million in grants to assist states or their designees to develop state-specific data on the deployment levels and adoption rates of broadband services. These data, including publicly available state-wide broadband maps, will also be used to develop the comprehensive, interactive national broadband map that NTIA is required by the Recovery Act to create and make publicly available by February 17, 2011.

The national broadband map will publicly display the geographic areas where broadband service is available; the technology used to provide the service; the speeds of the service; and broadband service availability at public schools, libraries, hospitals, colleges, universities, and public buildings. The national map will also be searchable by address, and broadband service providers will have the option to make their identity available.

While the BDIA mandates that each state may have only a single, eligible entity perform the mapping, each state's applicant will be carefully evaluated under the standards described in NTIA's Notice of Funds Availability. If an applicant does not meet the program standards, it will not receive funding and NTIA may perform the necessary broadband data collection. Applications were accepted through the online grants.gov system from July 14, 2009, at 8 a.m. EDT until August 14, 2009.

In Mississippi, the Office of the Governor led the effort to solicit proposals from qualified vendors interested in providing broadband mapping/deployment/adoption consulting and services for the Mississippi Broadband Task Force. This initiative will focus on conducting research/mapping to provide a comprehensive picture of current infrastructure deployment and availability in the State, working with providers to encourage build out in areas lacking accessibility, and engaging local community teams to analyze current use of broadband and educate on opportunities.

The Program will provide up to approximately $240 million in grants to assist states or their designees to develop state-specific data on the deployment levels and adoption rates of broadband services.

Going Virtual

By Craig P. Orgeron, Ph.D.
Director, Strategic Services

Current research suggests that key strategic initiatives for information technology energy management focus on implementing server and storage virtualization technologies and optimization of physical IT server facilities. By definition, these approaches require more time, effort, and up-front expenditures, but also have the greatest potential for long-term and substantial energy savings across state government.

Going Virtual

Continued from page two

The potential energy savings from virtualization are vast. Even when operating at only 5% of capacity, a server uses 90% of allocated power. On average, a typical server uses 23.8 kW/day. With cooling and power demands remaining continuous, even as servers are idle, nearly half of all operational costs for servers are expended on power and cooling needs. Thus, by streamlining the number of physical servers, floor space is reduced, and cooling and capital costs are also reduced, while the utilization of servers increases – all lending to lower energy consumption. For every 10 servers virtualized, roughly $14,300 of energy savings are expected annually.

Virtualization is a proven technology and offers many benefits to the State of Mississippi. However, virtualization software is not plug-and-play and must be installed and configured by experienced personnel. A deliberate, planned approach for implementing a virtualization solution across state government must be developed and followed to maximize the benefits, minimize the cost, and ensure continuity of service within each agency. As a first step, IT assets must be accurately inventoried and a virtualization plan for servers, inclusive of time and cost estimates per agency, must be developed. The plan will need to include specific hardware and software recommendations for each agency. As a general guideline, the virtualization of 100 servers, from inception to completion, requires six months.

The Mississippi Department of Information Technology Services (ITS) is in the process of awarding a contract to a single VMware Certified Professional (VCP) vendor with either a VIP Enterprise or higher level certification to provide server virtualization consulting services. The awarded vendor will enter into a Master Services Agreement and must will a statement of work for each state agency requesting server virtualization services. This awarded RFP will be used on an as-needed basis by state agencies seeking to virtualize and migrate their private servers into the ITS Virtual Data Center's environment located at either the Robert E. Lee Building and/or ITS' new Data Center on Lakeland Drive. Even though state agencies will be the primary customer base, other state entities may use this awarded RFP. The virtualized server location will be determined at the time of the request. The Mississippi Department of Human Services (MDHS) will be the first state agency to leverage server virtualization services offered through ITS.

Data Center Update

By Mitchell Bounds
Director, Data Services

Relocation of Data Center to New Facilities

The Data Center staff is in the early stages of planning the relocation of Data Center operations to new facilities at the Lakeland Drive location. Two projects, discussed below, related to relocation will definitely involve customers of the Data Center. The Data Center staff will be requesting input from customers within the next six months to insure that this relocation process is as transparent as possible.

Conversion to Consolidated Tape Processing Platform

As many customers of the Data Center know, there are many different tape options available at the

Data Center Update
Continued from page three

Center. Options are sometimes good, but the expense and confusion of supporting the infrastructure has become an issue. Also, a large portion of the existing tape infrastructure is scheduled for End-of-Life June 2010. So as part of the Data Center relocation, the staff will implement a consolidated tape processing solution within the next six months. The solution likely will be comprised of virtual tape backed by physical tape media and a smaller set of direct addressable physical tape drives for offsite and disaster recovery requirements. The vendor has not been chosen yet, so details of the conversion are not available. There will be some impact to customers who use the tape infrastructure. However, there are many techniques that can be used to minimize impact to the customer and no large scale JCL or procedural changes are anticipated.

Conversion to Consolidated Disk Storage Platform

While not as visible to the customer as tape processing, external disk storage at the Data Center is also a hodgepodge of equipment. The staff will be converting the present environment to consolidated high-end storage sub-systems with SAN and direct connection options. Although the process of moving data is quite involved, the Data Center has proven technology to move large amounts of data "on the fly" without affecting applications. Under no circumstances will data be moved without the knowledge or participation of the owner of the data.

Access to Mainframe from Internet

Direct access from the Internet to the mainframe using TN3270 clients without a VPN or Host on Demand (HOD) will no longer be allowed after September 30, 2009. If a customer needs access to mainframe applications through an Internet connection, either a VPN must be requested through ITS or the customer may use the HOD system provided by the Data Center. HOD is an application that uploads a TN3270 emulator to a Web browser and provides support for SSL security. If you need a VPN or HOD setup, it can be requested by calling the ITS Service Desk at 601-359-5959.

Some Y2K Remediation Concerns

There have been some concerns about Y2K remediation popping up here and there on the Web and in trade publications. If temporary patches using some kind of pivot year were put into applications that were supposed to be replaced before 2010, but the applications are still being used, a second look at these applications may be advisable. If data field expansion was the remediation option, there should be no further issues.

Information Security Division at ITS

By Craig P. Orgeron, Ph.D.
Director, Strategic Services

In June 2009, the Information Security Division (ISD), a new division within Information Technology Services (ITS) was launched. The ISD was created as a result of direction from the ITS Board to establish a focal point within ITS for a renewed, strategic emphasis on information security across all state agencies. This renewed security effort will strongly emphasize full cooperation, cohesive planning and collaborative efforts among state agencies. It will also be supported by the State Auditor's Office who will work closely with ISD to establish, review, and ensure compliance with enterprise security policies that are based upon evolving industry standards and best practices.

Information Security Division at ITS

Continued from page four

With extensive expertise in networking and the management of IT resources and contracts, Jimmy Webster has been tapped to serve as Director of the ISD, and in that role he will also serve as the State's Chief Information Security Officer. Jimmy will be assisted by two experienced ITS staff members in the new ISD: Jay White, security analyst, who will work closely with the state agencies in the areas of general security planning and compliance; and Greg Nohra, security engineer, who will continue to function as the security engineer responsible for core and perimeter defense systems while also working with agencies on specific technical security challenges.

The Information Security Division will be responsible for developing and maintaining an enterprise security plan for information technology security and for reviewing this plan with the ITS Executive Director and Board annually. To this end, ISD will engage relevant efforts in federal government, other states, and industry as part of its responsibility for state-wide information security including rulemaking and policy, audit oversight, education and awareness programs, and coordination and compliance for security planning, reporting, and incident response.

The ITS Executive Director and Board and are committed to effective implementation of a collaborative, consistent information security environment across all state agencies – an environment which is intended to mitigate the severe and growing security threats which have the very real potential to disrupt major elements of the missions of our state agencies.

For information regarding ISD, contact Jimmy Webster via e-mail (jimmy.webster@its.ms.gov), or by phone at 601-359-2690.

Cybercrime

Provided by: Multi-State Sharing and Analysis Center
www.msisac.org

What is Cybercrime?

The term "cybercrime" is usually referred to as any criminal offense committed against or with the use of a computer or computer network. The US Department of Justice (DOJ) interchangeably uses the terms "cybercrime," "computer crime," and "network crime" to refer to acts such as computer intrusions, denial of service attacks, viruses and worms.[1] A cybercrime incident can lead to loss of business and consumer confidence, financial loss, productivity loss, and even loss of intellectual property. For something to be considered a crime, however, requires a law to denote it as such, and the laws have, to this point, lagged behind technology. Existing laws relating to cybercrime oftentimes do not apply to specific acts being investigated and those laws vary from state to state. Some cybercrime may be more easily prosecuted if it is simply viewed as a more commonly recognized crime, e.g. vandalism instead of web defacement. To refer to a criminal act as "cybercrime" or "computer crime" tends to place the focus more on the technology, rather than on the crime itself. For these reasons, Anthony Reyes, author of the book *Cyber Crime Investigations*, argues against using the term "cybercrime," and instead prefers to call these acts as "crimes with a computer component."[2] Regardless of the means used to commit a crime or the target of a crime, whether it is a computer, a business, or someone's data, it is still a crime.

What are the Trends in Cybercrime?

In the 1990s, cybercrime was mainly motivated by notoriety or revenge and predominately defined by the willful destruction of online property or intentional disruption of a business. The current era of cybercrime is dominated by criminals who want to use your computer for illegal activities, to steal

Cybercrime

Continued from page five

data for profit, and organized crime is heavily involved.[3] Attackers exploit vulnerabilities in computer software in order to develop "crimeware," such as viruses, Trojans, and keyloggers, in order for other criminals to carry out their nefarious acts. These "crimeware" creators also utilize the software-as-a-service business model to provide crimeware-as-a-service. Some of their crimeware servers not only act as command and control servers (machines designed to provide instructions to the crimeware), but also as "data suppliers" or repositories for private stolen information that is harvested by the crimeware. Personal information is a valuable commodity for criminals. Traditional security tools are becoming increasingly more limited in their ability to mitigate these highly complicated cybercrime attacks.[4] Another trend is that the governments of various countries are suspected of being involved in cybercrimes for political reasons. As governments become more dependent upon technology, those assets will be attacked for various reasons. The cybercrime landscape, as it may be called, has definitely changed, but the criminal motivations are still the same – money, power and revenge.

What Can I Do?

Fighting cybercrime is problematic for several reasons. Many actions, such as writing crimeware, are currently not defined as illegal and, even if they constitute a crime, can be difficult to prosecute. Location and jurisdiction may also be a problem. For instance, a criminal may reside in one country and use a crimeware server in another country to attack a victim who resides in a third country.[5] Cybercrime can also be perpetrated without a person's knowledge, unlike other types of crimes that may be more noticeable. To adequately defend against cybercrime, you need against cybercrime, you need to follow the traditional best practices for protecting your network or desktop.

If you become a victim of cybercrime, you should report the incident to the appropriate law enforcement authorities. Depending on the scope of the crime, the appropriate agency may be local, state, federal, or even international. The US DOJ maintains a list of federal agencies to which computer related crimes may be reported at the following address: http://www.usdoj.gov/criminal/cybercrime/reporting.htm. In addition, you may report cybercrimes to the Internet Crime Complaint Center (IC3), a partnership among the Federal Bureau of Investigation (FBI), the National White Collar Crime Center (NW3C) and the Bureau of Justice Assistance (BJA). The IC3 provides a convenient reporting mechanism for both citizens and government agencies that alerts authorities of suspected criminal or civil violations and may be contacted via the following address: http://www.ic3.gov.

[1] "Prosecuting Computer Crimes", February 2007, http://www.usdoj.gov/criminal/cybercrime/ccmanual/00ccma.html.
[2] Reyes, Anthony, Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors, Syngress Publishing, Inc. 2007.
[3] "A Brief History of Data Theft", The ISSA Journal, June 2008.
[4] "The Cybercrime 2.0 Evolution", The ISSA Journal, June 2008.
[5] Organized Cybercrime", The ISSA Journal, October 2008.

FOR YOUR INFORMATON
Published by:
Mississippi Department of Information Technology Services
Contact: Caren Brister
601-359-9598
caren.brister@its.ms.gov